

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-187009

(43)Date of publication of application : 09.07.1999

(51)Int.Cl.

H04L 9/08

G09C 1/00

G09C 1/00

(21)Application number : 09-349167

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 18.12.1997

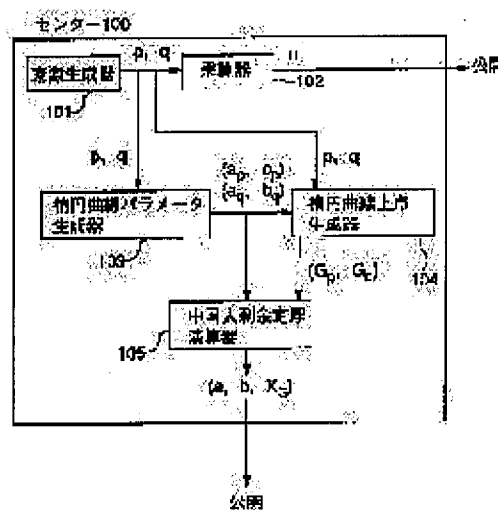
(72)Inventor : OKAMOTO TATSUAKI
UCHIYAMA SHIGENORI

(54) NON-COMMUNICATION KEY DELIVERING METHOD, EQUIPMENT THEREFOR AND PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a non-communication key delivering system without a threshold value, of a simple algorithm and of good efficiency by utilizing a special elliptic curve on which the discrete logarithm is easily calculated.

SOLUTION: A center 100 can easily calculate the discrete logarithm of the elliptic curve E_n on $n=pq$ (obtaining SA satisfying $SA \cdot G = h(IDA, rA)$ from $G, h(IDA, rA)$ as it knows prime numbers (p) and (q)). In addition, as SB generated similarly to SA, $h(IDB, rB) = SB \cdot G$. Consequently, $SA \cdot h(IDB, rB) = SA \cdot (SB \cdot G) = (SA \cdot SB) \cdot G = SB \cdot (SA \cdot G) = SB \cdot h(IDA, rA)$. Thus, a key KAB which a user A calculates from his secret key SA and the identifier IDB of a user B and a key KBA which the user B calculates from his secret key SB and the identifier IDA of the user A are coincident with each other.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-187009

(43) 公開日 平成11年(1999) 7月9日

(51) Int.Cl. ⁶	識別記号	F I
H 0 4 L 9/08		H 0 4 L 9/00 6 0 1 D
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00 6 2 0 A
		6 2 0 Z
	6 3 0	6 3 0 D

審査請求 未請求 請求項の数14 O L (全 6 頁)

(21) 出願番号 特願平9-349167

(22) 出願日 平成9年(1997)12月18日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 岡本 龍明

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(72) 発明者 内山 成憲

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 弁理士 草野 卓

(54) 【発明の名称】 無交信鍵配送方法、その装置、及びプログラム記録媒体

(57) 【要約】

【課題】 しきい値がなく、処理アルゴリズムが単純で効率が良い。

【解決手段】 センターTで素数 p 、 q から $p \times q = n$ を作り、 n を法とする環上での楕円曲線 E_n のパラメータ a 、 b と E_n 上の点の座標 G を作り、 a 、 b 、 G 、 n を公開し、 p 、 q を秘密に保持し、利用者Aの ID_A と整数 r_A とより $X = h(ID_A, r_A)$ を求め(106)、 $X^3 + aX + b \bmod n$ が平方剰余となる最小の r_A を求め(107)、その X を用いた $Y^2 = X^3 + aX + b \bmod n$ 点を $F = (X, Y)$ とし、この F に対し剰余演算を行い(108)、更に $s_A * G = F$ を満す s_A を求め(105)、 s_A をAの利用者鍵とし、AがBと通信する際には、同様の条件を満す $h(ID_B, r_B)$ を求め、 $s_A * h(ID_B, r_B)$ を共通暗号鍵とする。

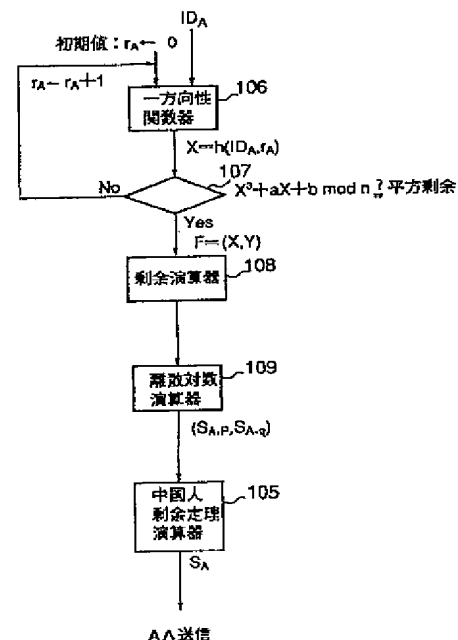


図 3

【特許請求の範囲】

【請求項 1】 鍵生成センター装置と多数の利用者 A、B、…、の利用者装置とからシステムが構成され、システムの初期設定段階において、鍵生成センター装置は合成数 n と n を法とする剰余類環上での楕円曲線 E_n のパラメータ及び E_n 上の点 G をシステムの共通パラメータとし公開し、 n の素因数を鍵生成センター装置に秘密鍵として秘密に保存し、利用者鍵の生成段階において、鍵生成センター装置は、利用者 A の識別子 ID_A から関数 F を用いて $F(ID_A)$ を計算し、上記秘密鍵を用いて、楕円曲線上の演算 $s_A * G = F(ID_A)$ を満足する利用者鍵 s_A を計算し、 s_A を利用者 A の利用装置に秘密に配送し、無交信鍵配送段階において、利用者 A がその利用者装置と利用者 B の利用者装置とにより利用者 B と交信する際に、利用者 A の利用者装置は利用者鍵 s_A と利用者 B の識別子 ID_B から $s_A * F(ID_B)$ を計算し、利用者 B との共通の暗号鍵 K_{AB} とすることを特徴とする無交信鍵配送方法。

【請求項 2】 上記利用者 A の利用者鍵の生成は、識別子 ID_A と整数 r_A との連結を変数とする一方向性関数値 X が上記楕円曲線上の点の x 座標となる最小の整数 r_A を求め、その条件を満たす楕円曲線の点を剰余演算して上記 $F(ID_A)$ を求めることを特徴とする請求項 1 記載の無交信鍵配送方法。

【請求項 3】 上記共通暗号鍵 K_{AB} の生成において、上記識別子 ID_B と整数 r_B との連結を変数とする一方向性関数値が上記楕円曲線の点の x 座標となる最小の整数 r_B を求めて上記 $F(ID_B)$ を得ることを特徴とする請求項 1 又は 2 記載の無交信鍵配送方法。

【請求項 4】 自己の利用者鍵 s_A を保持する手段と、通信相手 B の識別情報 ID_B と、公開されている楕円曲線 E_n のパラメータとその曲線 E_n 上の公開されている点 G とから $F(ID_B)$ を計算する手段と、上記 $F(ID_B)$ と上記利用者鍵 s_A との上記楕円曲線 E_n 上での加算演算 $s_A * F(ID_B)$ を計算して上記通信相手 B との共通の暗号鍵 K_{AB} を得る手段とを具備する無交信共通暗号鍵生成利用者装置。

【請求項 5】 上記点 $F(ID_B)$ 計算手段は、上記識別情報 ID_B と整数 r_B の連結を変数とする一方向性関数値を求める関数演算手段と、上記求めた一方向性関数値を変数とし、上記楕円曲線のパラメータ、公開情報 n を法とする値 Z を求める剰余演算手段と、上記値 Z が n を法とした平方剰余である最小の上記整数 r_B を求める手段と、よりなることを特徴とする請求項 4 記載の無交信共通暗号鍵生成利用者装置。

【請求項 6】 上記最小の r_B を求める手段は、上記値 Z が $(Z/n) = 1$ であるか否かを検査するヤコビ記号

演算手段と、

上記一方向性関数値を x 座標とする点を上記楕円曲線上で n 回加算すると無限遠点になるか否かを検査する楕円曲線上加算手段と、

上記ヤコビ記号演算手段の検査が 1 であり、かつ上記楕円曲線上加算手段の検査で加算値が無限遠点になることを満たすまで上記整数 r_B を 0 より順次大とする手段と、よりなることを特徴とする請求項 5 記載の無交信共通暗号鍵生成利用者装置。

10 【請求項 7】 無交信で共通暗号鍵を生成するために利用者装置で実行するプログラムを記録した記録媒体であって、

上記プログラムは、

通信相手 B の識別情報 ID_B と、公開されている楕円曲線 E_n のパラメータと、その曲線 E_n 上の点の座標とから、楕円曲線 E_n 上の点 $F(ID_B)$ を計算する過程と、

上記 $F(ID_B)$ と自己の秘密鍵 s_A との楕円曲線 E_n 上での加算演算 $s_A * F(ID_B)$ を行い共通暗号鍵 K_{AB} を得る過程と、

20 を行うことを特徴とするコンピュータ読出し可能な記録媒体。

【請求項 8】 上記点 $F(ID_B)$ を計算する過程は、上記識別情報 ID_B と整数 r_B の連結を変数とする一方向性関数値を求める過程と、

公開情報 n を法として、上記求めた一方向性関数値を変数とし、上記楕円曲線 E_n の関数値 Z を求める過程と、上記値 Z が n を法とした平方剰余である最小の整数 r_B を求める過程とよりなることを特徴とする請求項 7 記載の記録媒体。

30 【請求項 9】 上記最小の r_B を求める過程は、上記値 Z が $(Z/n) = 1$ か否かを検査するヤコビ記号演算過程と、

上記一方向性関数値を楕円曲線 E_n 上で n 回加算する無限遠点になるかを検査する楕円曲線上加算過程と、

上記ヤコビ記号演算過程の検査が 1 であり、かつ上記楕円曲線上加算過程の検査で加算値が無限遠点になることを同時に満たすまで上記整数 r_B を 0 から順次大とする過程とよりなることを特徴とする請求項 8 記載の記録媒体。

【請求項 10】 合成数 n を生成し公開する手段と、 n を法とする環上での楕円曲線 E_n のパラメータ及び E_n 上の点 G を生成して公開する手段と、上記 n の素因数を秘密鍵として秘密に保持する手段と、利用者 A の識別子 ID_A から関数 F を用いて $F(ID_A)$ を計算する手段と、上記秘密鍵を用いて、楕円曲線 E_n 上の演算 $s_A * G = F(ID_A)$ を満足する s_A を計算する手段と、

上記 s_A を上記利用者 A の秘密鍵としてその利用者装置に秘密に配送する手段とを具備する無交信鍵配送センタ

一装置。

【請求項11】 上記 $F(ID_A)$ を計算する手段は、
上記 ID_A と整数 r_A の連結を変数として一方方向性関数
値 $X=h(ID_A, r_A)$ を求める手段と、
上記 X を変数として上記楕円曲線 E_n に代入したものが
平方剰余を満たす最小の整数 r_A を求める手段と、
上記最小の整数 r_A にもとづく上記 X を上記楕円曲線 E_n
に代入しかつ法 n の剰余演算を満たす点を求めて上記 F
(ID_A)を得る手段とよりなることを特徴とする請求
項10記載の無交信鍵配送センター装置。

【請求項12】 多数の利用者 A, B, \dots 、に対し、利
用者間で交信することなく鍵を配送する無交信鍵配送セ
ンター装置で実行するプログラムを記録した記録媒体で
あって、

上記プログラムは、

合成数 n を生成し公開する過程と、

n を法とする環上での楕円曲線 E_n のパラメータ及び E_n
上の点 G を生成して公開する過程と、

上記 n の素因数を秘密鍵として秘密に保持する過程と、
利用者 A の識別子 ID_A から関数 F を用いて $F(ID_A)$
を計算する過程と、

上記秘密鍵を用いて楕円曲線 E_n 上の演算 $s_A * G = F$
(ID_A)を満足する s_A を計算する過程と、

上記 s_A を上記利用者 A の利用者鍵としてその利用者装
置へ秘密に配送する過程とを行うコンピュータ読出し可
能な記録媒体。

【請求項13】 上記 $F(ID_A)$ を計算する過程は、
上記 ID_A と整数 r_A の連結を変数として一方方向性関数
値 $X=h(ID_A, r_A)$ を求める過程と、
上記 X を変数として上記楕円曲線 E_n に代入した値が平
方剰余を満たす最小の整数 r_A を求める過程と、
上記最小の整数 r_A にもとづく上記 X を上記楕円曲線 E_n
に代入しかつ法 n の剰余演算を満たす点を求めて上記 F
(ID_A)を得る過程と、

を有することを特徴とする請求項12記載の記録媒体。

【請求項14】 上記 n を生成する過程は、素数 p, q
を生成する過程と、 p と q の積を求めて上記 n とする過
程とを有し、

上記パラメータ及び点 G を生成する過程は、上記 p 及び
 q に対し、それぞれ点の個数が p 及び q である楕円曲線
 $E_p(a_p, b_p)$ 及び $E_q(a_q, b_q)$ のパラメー
タ $(a_p, b_p), (a_q, b_q)$ を生成する過程と、
楕円曲線 E_p, E_q 上の点の G_p, G_q を求めて上記点
 G を得る過程とよりなることを特徴とする請求項12又
は13記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電気通信シス
テムにより暗号通信用の鍵を配送する鍵配送方法、特に利
用者間で交信することなく鍵を配送する無交信鍵配送方

法(岡本、山本著「現代暗号」産業図書)を実現する方
法、その装置、及びそのプログラム記録媒体に関する。

【0002】

【従来の技術】無交信鍵配送方式は、許容不正利用者数
にしきい値がある方式としきい値が無い方式に大別され
る(岡本、山本著「現代暗号」産業図書、13.5.2節)。し
きい値がある方式の代表例は、松本、今井によるKPS
(Matsumoto, T. and Imai, H.: On the Key Pre
distribution System: A Practical Solution to the
Key Distribution Problem, Proc. of Crypto'87, LNCS
293, Springer-Verlag, pp.185-193(1988))であるが、し
きい値があるため、一定数以上の利用者がそれぞれの秘
密鍵を持ち寄ると、それからシステム共通の秘密鍵が計
算でき、システム全体が崩壊する。

【0003】しきい値が無い方式の代表例は、辻井らに
よるNIXS-TAS(Tsujii, S., Araki, K., Kasahara, M.,
Okamoto, E., Sakai, R., Maeda, Y., and Yagisawa, T.:
On Ambiguity in Coppersmith's Attacking Method against
NIXS-TAS Scheme, IEEE Trans. Fundamentals, E79-A,
1, pp.66-75(1996))である。しかし、この方式は処理
アルゴリズムが大変複雑で、単に効率性に問題があるの
みならず、安全性の検証が困難である。

【0004】

【発明が解決しようとする課題】この発明の目的は、し
きい値が無く、処理アルゴリズムが単純で効率の良い無
交信鍵配送システム及びそのプログラム記録媒体を提供
することにある。

【0005】

【課題を解決するための手段】ある特殊な楕円曲線で
は、その上での離散対数が容易に計算できるが、この発
明では、そのような楕円曲線を利用することにより、無
交信鍵配送方式を効率的に実現する。

【0006】

【発明の実施の形態】図1に、この発明のシステム構成
例を示す。鍵生成センターの装置(以降、センターと呼
ぶ)100と、利用者の装置(以降、利用者と呼ぶ)200の複
数とがそれぞれ通信回線を介して接続している。

(1)システムの初期設定

図2を用いて、システムの初期設定処理の説明を行う。
センター100は、素数生成器101を用いて素数 p, q を生成
し、乗算器102を用いて、 $n=pq$ を計算し、さらに、 p, q
を楕円曲線パラメータ生成器103に入力してパラメータ
 $(a_p, b_p), (a_q, b_q)$ を出力する。ここで、生成された
楕円曲線 $E_p(a_p, b_p), E_q(a_q, b_q)$ はそれぞれ、点の
個数が p および q となっている。このような楕円曲線の
生成の具体的なアルゴリズムは文献(Miyaji, A.: Elliptic
Curves over F_p Suitable for Cryptosystem

s, Proc. of Auscrypt'92, LNCS, Springer-Verlag, pp.479-504(1993))に示されている。また、

$(a_p, b_p), (a_q, b_q)$ を楕円曲線上点生成器 104 に入力し、 (G_p, G_q) を出力する。 $(p, q), (a_p, b_p), (a_q, b_q)$ 及び (G_p, G_q) を中国剰余定理演算器 105 に入力し、 (a, b) 及び G の x -座標、 X_G を出力する。ここで、 $a \equiv a_p \pmod{p}, a \equiv a_q \pmod{q}, b \equiv b_p \pmod{p}, b \equiv b_q \pmod{q}, G \equiv G_p \pmod{p}, G \equiv G_q \pmod{q}$ であり、以降これらを $a = [a_p, a_q]$ などと表記する。

【0007】センター100は、 p, q を秘密鍵として保持し、 (n, a, b, X_G) を公開鍵として公開する。

(2) 利用者鍵の生成

図3を用いて、利用者鍵の生成処理の説明を行う。センター100は、以下の手順で、利用者A200の識別子 ID_A からAの秘密鍵 s_A を生成する。

【0008】まず、Aは、 $r_A = 0$ に対して、ハッシュ関数のような方向性関数の関数演算器106を用いて、 $X = h(ID_A, r_A)$ を計算し、さらに平方剰余判定器107を用いて $X^3 + aX + b \pmod{n}$ が平方剰余かどうか判定し、平方剰余ならば、つまり X が楕円曲線 E 上の点の x 座標となったので、その $Y^2 \equiv X^3 + aX + b \pmod{n}$ を満足する点を $F = (X, Y)$ とし、剰余演算器108を用いて、 $F_p = F \pmod{p}$ and $F_q = F \pmod{q}$ をそれぞれ演算する。もし、判定器107で平方剰余でないと判定すると、 r_A の値を1だけ増やし、同様の手続きを繰り返し行い、平方剰余となる最小の r_A を見つける。

【0009】次に、センター100は、離散対数演算器109を用いて、

$$s_{A,p} G_p = F_p, s_{A,q} G_q = F_q$$

を満たす $s_{A,p}, s_{A,q}$ を計算する。ここで、このアルゴリズムは文献 (Sato, T., and Araki, K.: Fermat Quotient and the Polynomial Time DiscreteLog Algorithm for Anomalous Elliptic Curves, Preprint (September, 1997), to appear in the Proceedings of PKC'98, LNCS, Springer-Verlag) に示されている。さらに、中国剰余定理演算器105を用いて $s_A = [s_{A,p}, s_{A,q}]$ を計算する。

【0010】センター100は、 (s_A, r_A) を利用者A200に秘密に送信する。

(3) 無交信鍵配送

図4を用いて、無交信鍵配送処理の説明を行う。利用者A200は、以下の手順で、利用者Bとの間の暗号鍵 K_{AB} をBと交信することなく生成する。まず、利用者Aは、以下の検査を行いこれらを同時に満足する最小の r_B ($r_B \geq 0$) を求める。

・関数演算器206及び剰余演算器201を用いて $Z =$

$h(ID_B, r_B)^3 + a h(ID_B, r_B) + b \pmod{n}$ を計算し、さらにヤコビ記号演算器202を用いて $(Z/n) = 1$ となるかどうかを検査する。ヤコビ記号の計算アルゴリズムは文献 (Knuth, D. E.: The Art of Computer Programming, Addison-Wesley Publishing Co., (1981)) 等に記されている。 $(Z/n) = 1$ ということは2分の1の確率で、上記Zの式が n を法とする平方剰余であることになる。

・楕円曲線の x -座標加算演算器203を用いて $n * h(ID_B, r_B) = \infty$ となるかどうかを検査する。なお、 $n * X$ は、楕円曲線 E_n のある点の x -座標である X に対して x -座標加算演算を n 回適用したものを意味する。この楕円曲線の x -座標加算演算の計算式は、文献 (Demytko, N.: A New Elliptic Curve Based Analogue of RSA, Proc. of Eurocrypt'93, LNCS 765, Springer-Verlag, pp.40-49(1994)) に示されている。つまり $n * h(ID_B, r_B) = \infty$ とは楕円曲線 E_n 上の点 $h(ID_B, r_B)$ を n 回加算演算した結果は無限遠点になる (この楕円曲線 E_n の位数は n) ことを意味する。

【0011】次に、 x -座標加算演算器203を用いて、利用者A200は、

$$K_{AB} = s_A * h(ID_B, r_B)$$

を計算する。

【0012】

【発明の効果】この発明では、センター100は素数 p, q を知っているため $n = pq$ 上での楕円曲線 E_n の離散対数 $(G, h(ID_A, r_A))$ より、 $s_A * G = h(ID_A, r_A)$ を満足する s_A を求めることが容易に計算できる。更に s_B も s_A と同様に作られたものであるから $h(ID_B, r_B) = s_B * G$ であり、従って $s_A * h(ID_B, r_B) = s_A * (s_B * G) = (s_A s_B) * G = s_B * (s_A * G) = s_B * h(ID_A, r_A)$ が成立するため、利用者Aが自分の秘密鍵 s_A と利用者Bの識別子 ID_B より計算した鍵 K_{AB} と、利用者Bが自分の秘密鍵 s_B と利用者Aの識別子 ID_A より計算した鍵 K_{BA} が一致する。つまり、利用者AとBは無交信で鍵を共有することが可能となる。

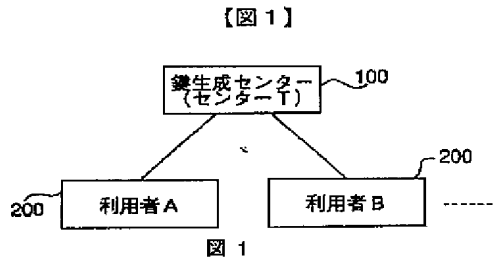
【0013】システムの初期設定における、センターで必要とされる処理は十分に効率的に実現が可能であり、パーソナルコンピュータで数分程度の時間で生成できる。詳しくは、文献 (Miyaji, A.: Elliptic Curves over F_p Suitable for Cryptosystems, Proc. of Auscrypt'92, LNCS, Springer-Verlag, pp.479-504(1993)) を参照されたい。

【0014】利用者鍵の生成における、センターで必要とされる処理も十分に効率的に実現が可能であり、一人の利用者の鍵生成に要する処理量は、鍵サイズの3乗のオーダーである (つまり、RSA暗号の復号程度の処理量である)。各利用者の無交信鍵配送に要する処理量も

鍵サイズの3乗のオーダーである。上記に示すように、この発明によれば、単純な原理に基づいており、その安全性の解析は比較的容易である。つまり、この発明の安全性は、楕円曲線 E_n が与えられて、 $(X, s * X, t * X)$ から $(s, t) * X$ を求める問題の難しさと同等である。

【図面の簡単な説明】

【図1】 この発明方法が適用されるシステムの構成例を

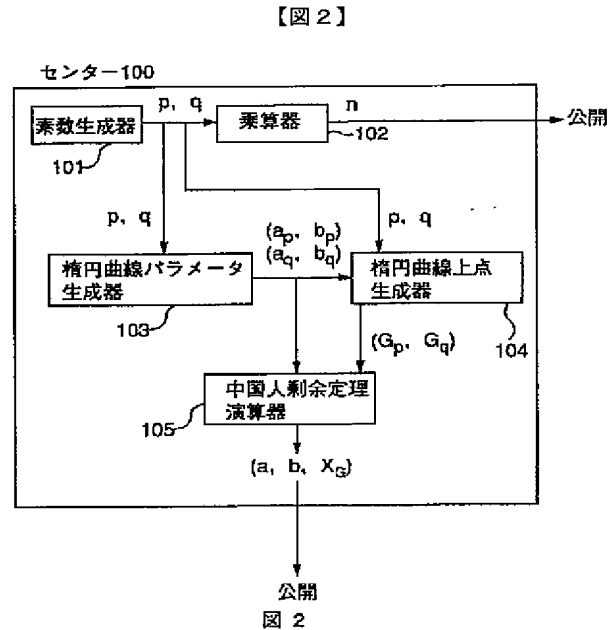


示すブロック図。

【図2】 センター装置におけるシステム初期設定時に行う処理に必要な機能構成例を示す図。

【図3】 センター装置における利用者鍵の生成に必要な機能構成例を示す図。

【図4】 利用者装置で無交信共通暗号鍵の生成に必要な機能構成例を示す図。



【図3】

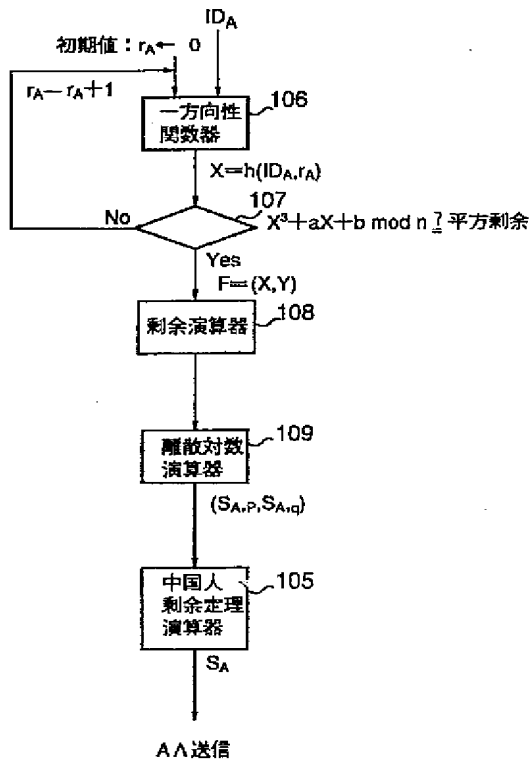


図 3

【図4】

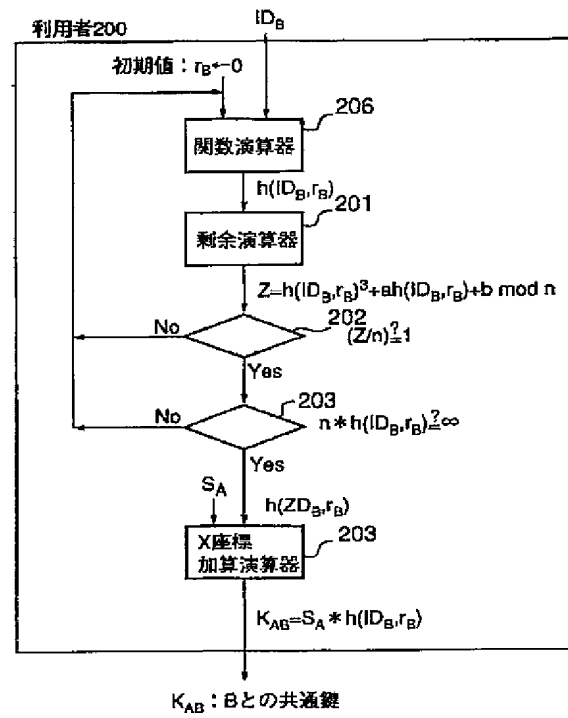


図 4